Bring Your Own Device (BYOD) to Collegium Charter School
Acceptable Use Statement and Parameters of a Pilot Program for Grades 9-12

Collegium Charter School (CCS) is dedicated to providing our students with the knowledge necessary to be a responsible digital citizen. We envision a learning environment where technology is *a part of* us, not *apart from* us.

Purpose:
CCS is committed to moving students and staff forward in a 21st century learning environment. As part of this plan, CCS will now allow high school students and staff to access the wireless network using their own technology devices (laptops, smartphones, iPads, etc.) during the school day. With teacher approval, students may use their own devices in the classroom to access and save information from the Internet, communicate with other learners, and use the productivity tools loaded on their devices.

CCS believes that the tremendous value of technology and the information technology network as an educational resource outweighs the potential risks associated with the use of technology by high school students. We will leverage existing and emerging technology as a means to learn and thrive in the 21st century and prepare our students for success toward their goals in the competitive global and electronic age. Access to the tools and resources of a world-wide network and understanding when and how these tools are appropriately and effectively used are imperative in each student's education.

Pilot Plan:
Beginning in the 2014-2015 school year, students in grades 9-12 may bring their own technology devices to school as part of a pilot program.

Before attempting to connect to our BYOD network, users must acknowledge and accept the following terms of use: CCS is providing wireless connectivity as an optional service and offers no guarantees that any use of the wireless connection is in any way secure, or that any privacy can be protected when using this wireless connection. Use of the CCS wireless network is entirely at the risk of the user, and CCS is not responsible for any loss of any information that may arise from the use of the wireless connection, or for any loss, injury or damages resulting from the use of the wireless connection. Users are advised to take appropriate steps to protect their devices from unauthorized users and viruses. All users of the BYOD network are bound by this *BYOD Acceptable Use Statement and Parameters* and the Collegium *Student Code of Conduct*. Once on the network, all users will have filtered Internet access just as they would on a school-owned device.

The school's information technology resources, including email and Internet access, are provided for educational purposes. If a student has any doubt about whether a contemplated activity is acceptable, consult with a teacher or other CCS employee to help determine if a use is appropriate. Adherence to the parameters listed below is necessary for continued access to the school's technological resources:

Student users must respect and protect the privacy of others:

- Access only assigned accounts.
- Only view, use, copy, and/or distribute authorized data and/or networks.
- Only take, use, copy, and/or distribute photos/videos of others with their permission.
- Refrain from distributing private/confidential information about others or self.

Student users must respect and protect the integrity, availability, and security of all electronic resources by:

- Observing all school Internet filters and posted network security practices.
- Reporting security risks or violations to a teacher or other CCS employee.
- Not destroying or damaging data, networks, or other resources that do not belong to them.
- Conserving and protecting shared resources.
- Not creating WiFi hotspots with their device on campus.
- Protecting passwords and account information. Students may not share passwords/account information with other students.
- Notifying a teacher or other CCS employee of network malfunctions.

Student users must respect and protect the intellectual property of others by:

- Following copyright laws (not making illegal copies of music, games, movies, etc.).
- Citing sources when using others' work (not plagiarizing).

Student users must respect and practice the principles of community by:

- Communicating only in ways that are kind and respectful.
- Reporting threatening or troubling materials to a teacher or other CCS employee.
- Not intentionally accessing, transmitting, copying, or creating material that violates Collegium's *Student Code of Conduct* (ex. messages/content that are pornographic, threatening, rude, discriminatory, harassing, bullying, etc.).
- Not intentionally accessing, transmitting, copying, or creating material that is illegal (ex. obscenities, stolen materials, or illegal copies of copyrighted works).
- Not using the resources to further other acts that are criminal or violate Collegium's *Student Code of Conduct*.
- Avoiding spam, chain letters, or other mass unsolicited mailings.
- Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

Users may, if in accord with the policy above:

- Use the resources for educational purposes.
- Design and post webpages and other material from school resources.
- Communicate electronically via tools such as email, chat, text, or videoconferencing.
- Install or download software, if also in conformity with laws and licenses, (students must be under the supervision of a CCS employee).
- Use electronic devices for nonverbal, non-disruptive use during non-instructional times in locations designated by the administration.

- Use of electronic devices or photography and/or recording when authorized by the building principal or designated professional staff member for the purposes of participation in educational activities.
- Communicate with social media and utilize social networking online tools and services. Students will be held accountable for the content of the communications that they state/post on social media.

Consequences for Violation:

Violations of these rules may result in disciplinary action, and could include the loss of a user's privileges to use Collegium's information technology resources. Further discipline may be imposed in accordance with the *Student Code of Conduct* up to and including suspension or expulsion depending on the degree and severity of the violation(s).

Supervision and Monitoring:

The use of Collegium's information technology resources is not private. School administrators and authorized employees have the ability to monitor the use of information technology resources to help ensure that users are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will if available, furnish evidence of crime(s) to law enforcement. If a parent/guardian does not want their child to have Internet access, the parent/guardian must notify their child's Principal in writing (via email suffices).

Bring Your Own Device (BYOD) to Collegium Charter School
Acceptable Use Statement and Parameters of a Pilot Program for Grades 9-12

I have read the *BYOD Acceptable Use Statement and Parameters* and agree to adhere to the standards provided in the document. I understand that as a user of the BYOD network I am bound by this *BYOD Acceptable Use Statement and Parameters* and the Collegium *Student Code of Conduct*. I also understand that failure to follow the *BYOD Acceptable Use Statement and Parameters* and the Collegium *Student Code of Conduct* will result in consequences in accordance to the *BYOD Acceptable Use Statement and Parameters* and the Collegium *Student Code of Conduct*.

Student Name: _____

Student Signature: _____

Date: _____

Please return to the 535 Main Office.

FAQs - BYOD (Bring Your Own Device)
Student, Parent/Guardian, and Employee Guide

Students

Q: I brought my iPad to school to use in the classroom, but my teacher said I couldn't use it in her classroom. Can I still use it?
A: The teacher in the classroom has the final say on procedures in the classroom. If he or she tells you not to use your device, then you must follow those directions. Access is only available, not guaranteed, for each classroom situation.

Q: I need to save my work in my CCS shared folder. Why can't I access this resource?
A: You are on the BYOD Network. It is not the same as the network you would normally access from a building computer. You will not see your shared folder, so you will need to save your work on your device.

Q: I need to print the spreadsheet I just created. Why is there no printer listed when I try this?
A: Like the shared folders, printers are on the CCS network and will not be available when you login to the BYOD network. A printing solution could include: saving the spreadsheet to a flash drive or using a web-based application (ex. Google Drive, Dropbox, Evernote, etc.) and printing from home or CCS computer. Keep in mind that using building printers in the classroom or other learning spaces is at the discretion of the teachers or other CCS employees.

Q: My laptop was stolen when I brought it to school. Whom should I contact about this?
A: Bringing your own technology device to school can be useful; however some risks are involved as well. It is always a good idea to record the device's serial number in case of theft. CCS is not responsible for the theft of a device, nor are we responsible for any damage done to the device while at school. Any time a theft occurs, you should immediately contact your Principal/Assistant Principal to report the missing device. To protect devices, students are encouraged keep their devices with them at all times or to secure in their locked locker.

Q: Why am I filtered on my own computer? Shouldn't I be able to see what I want to on my own device?
A: Student filtering is required by federal law of all public schools. The Children's Internet Protection Act (CIPA) requires all network access to be filtered, regardless of the device you use to access it while in a public school. The network you are using while at school belongs to CCS and will be filtered.

Q: Am I still held accountable for the *BOYD Acceptable Use Statement* (AU) and *Student Code of Conduct* even though this is my own personal computer?
A: Yes. The AU and Code of Conduct remain in effect even when you are using your own laptop, smartphone, iPad, etc. Each time you attempt to access the network at school you will be prompted to accept the terms of service that include the AU. Violating the terms of the AU would be a *Student Code of Conduct* violation.

Q: Why can't my little brother bring his laptop to school? He is in 8th grade.
A: Currently, we are limiting this privilege to high school students only.

Q: Am I able to connect my laptop to an open network port and gain access to the Internet?
A: No. CCS is only providing access to personal devices through the BYOD wireless network.

Q: Will there be a penalty to my grade if I do not have my own device?
A: No. Devices are not required and therefore, your grade will not be impacted.

PARENTS

Q: My son is bringing his iPad to school for instructional purposes. Will he have access to things he normally does with school equipment?
A: Your son will have access to any of the web-based software that the high school currently uses (databases, library search tools, etc.). Software may run differently on different devices for varying reasons. You should consult your owner's manual for software limitations. (Ex., iPads cannot run software requiring Flash Player.)

Q: As a parent, am I required to add additional software (virus protection, filter, tracking device, etc.) to my child's technology device?
A: No. Currently we do not require any additional software for school use. Virus protection is always advised, but not required to participate in the pilot. While on the CCS BYOD network, Collegium's filter will be in effect.

Q: If my daughter's laptop is stolen or damaged, what recourse can I take?
A: CCS is not responsible for any damage or theft of student-owned equipment. Installing tracking software can help locate the equipment if it is stolen, and keeping track of the device's serial number, model, and type will be helpful as well. Theft or vandalism of any kind should be reported immediately to the Principal/Assistant Principal. Theft or vandalism may also be reported to law enforcement. To protect devices, students are encouraged keep their devices with them at all times or secure in their locked locker.

Q: What are the building/classroom rules for using student-owned devices including phones?
A: Teachers/employees make the final decision for any tools used in the classroom; student owned equipment is no different. It will be up to the individual CCS employees to communicate their expectations to parents and students.

Q: Will my child have access to communication tools like email or message boards while on the BYOD network?
A: Yes. Students do have access to their email accounts.

CCS Employees

Q: Do I, as a CCS employee, have the choice when students can use their technology devices?

A: Students may use technology at the discretion of a CCS employee as a lesson or situation warrants.

Q: Some of my students cannot access the network on their laptops or phones. I don't have time in a class period to help them gain access. Should I put in a help request?

A: No. Students who cannot access the CCS BYOD wireless network, or who may have technical issues with their technology tool, need to take care of this issue outside of the classroom by working with their device's user manual. These are not CCS devices, and the school is not allocating resources to troubleshoot issues. It is not a staff member's responsibility to ensure that student-owned technology is functioning properly.

Q: I have students in my class who are accessing the Internet using their provider's data plan (AT&T, Sprint, Verizon etc.) on their smart phones or laptops, hence bypassing the filter. Is this a violation of the student AUP?

A: This is not an AUP violation because the student is not bypassing the filter on the CCS network, but instead using a provider's data plan. However, students must still follow the BYOD Acceptable Use Statement, the CCS Network Usage Policy (in the *Student Code of Conduct*), and the *CCS Student Code of Conduct*.

Q: One of my students was using his laptop while on campus to bully another student. Should I call the IT department concerning this problem?

A: No. Any disciplinary infractions that occur from using technology tools should be referred to the Principal/Assistant Principal immediately. This is a *Student Code of Conduct* violation.

Q: Should I call the IT department if one of my students' laptops is damaged or stolen?

Answer: No. Direct the student to report the theft/damage to the Principal/Assistant Principal. CCS is not responsible for any damage or theft of student-owned technology tools. It would be good to remind students to keep a record of the device's serial number.